PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60

A1

(11) International Publication Number: **WO 00/46725**

(43) International Publication Date: 10 August 2000 (10.08.00)

(21) International Application Number: PCT/US00/03017

(22) International Filing Date: 3 February 2000 (03.02.00)

(30) Priority Data:
09/245,790 5 February 1999 (05.02.99) US

(71) Applicant: FUNDSXPRESS, INC. [US/US]; 11950 Jollyville Road, Austin, TX 78759–2309 (US).

(72) Inventors: BURNS, John, A.; 6505 Danwood Drive, Austin, TX 78759 (US). LOWELL, Charles, M.; 3308 Rivercrest Drive, Austin, TX 78727 (US). BHAKTA, Rakesh, S.; 13408 Capadocia Cove, Austin, TX 78727 (US). HARTMAN, Sam, D.; 9014 Blue Quail Drive, Austin, TX 78758 (US).

(74) Agent: CAYWOOD, Michael; Locke Liddell & Sapp, LLP, Suite 300, 100 Congress Avenue, Austin, TX 78701 (US).

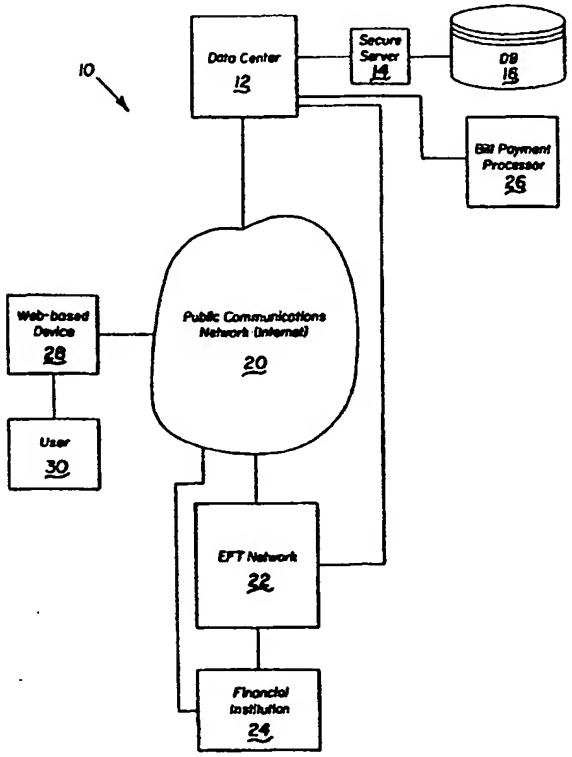
(81) Designated States: AU, CA, JP, MX, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM AND METHOD FOR CONDUCTING ONLINE FINANCIAL TRANSACTIONS USING ELECTRONIC FUNDS TRANSFER AND PUBLIC COMMUNICATIONS NETWORKS

(57) Abstract

An online financial transaction system and method which uses existing public communications network (item 20, figure 1) and an EFT network (item 22) to enable financial transactions by a customer (item 30) in a secure manner without transmitting the customer's PIN. The system includes a data center (item 12) with secure server (item 14) and database (item 16) wherein the data center is connected to the communications network (item 20) and to the EFT network (item 22). Also included in the system is a user interface (item 28) connecting authorized user (item 30) to the communications network (item 20). After establishing the connection, the user (item 30) enters an encrypted session with the secure server (item 14). Next, the user logs into the secure server (item 14) using an access ID and password. Once validated, the user (item 30) is able to conduct an online financial transaction without transmitting the user's PIN over the network (item 20).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SYSTEM AND METHOD FOR CONDUCTING ONLINE FINANCIAL TRANSACTIONS USING ELECTRONIC FUNDS TRANSFER AND PUBLIC COMMUNICATIONS NETWORKS

TECHNICAL FIELD

This invention relates to an online financial transaction system and method, and more particularly to a system and method for account inquiry, funds transfer and bill payment using existing electronic funds transfer and public communications networks without the need to transmit a personal identification number ("PIN") over the public communications network..

BACKGROUND OF THE INVENTION

With the rapid growth in popularity of the Internet, it has become almost a necessity for banks and other financial institutions to be able to offer their customers the ability to conduct basic financial transactions, such as account balance inquiry, transfer of funds between accounts and electronic bill payment, without the assistance of a teller. This ability permits the financial institution customer to perform financial transactions at the customer's convenience rather than during normal business hours. In order to meet this need some financial institutions have instituted voice activated telephone response systems which allow the customer to call the financial institution and conduct financial transactions after entering an ID and validating password. In one existing version of such a telephone system, the computer system on which the enabling software resides is connected to an electronic funds transfer ("EFT") network, sometimes referred to as an automated teller machine ("ATM") network. Valid financial transaction requests entered by the customer through the telephone system are then processed through the existing EFT network in a conventional manner. A disadvantage of this system is the requirement to use specialized telephone equipment having a display. In addition, certain information (account numbers, personal identification numbers ("PIN"s), etc.) that is normally encrypted and stored on the back of an ATM card in the magnetic stripe is needed for the transaction. Because the customer is using the telephone and no card reader is present, the customer is unable to transfer the encrypted information during the telephone call. Instead, the information must be stored and maintained on a computer system controlled by the financial institution or EFT network. The stored information must then be combined with the transaction information obtained

from the customer over the telephone and formatted into a request messaging stream capable of being interpreted by the EFT network. The disadvantage of such a system is that financial institutions using this system must convey sensitive customer account number and password information to the third party vendor maintaining the computer system which processes the requests received via telephone from participating financial institution customers. This transfer and storing of sensitive financial information to and by a third party poses a potential security risk.

Another popular method for banking without a teller is through online banking services. As more and more financial institutions offer such services to their customers, there is increased pressure on small financial institutions such as, for example, community banks, not currently offering similar online services to add them in order to compete effectively in the marketplace. In a typical online banking system, the financial institution hosts its web site on the financial institution's own computer system. In order to do this, the bank must purchase hardware such as a server, secure routers, and Internet connections. It must then develop custom online banking software. Large financial institutions with the requisite monetary and technical support resources were the first to offer online banking services to their customers. Because the process of adding online banking services is very involved technically and security of the system is always a concern, the larger financial institutions were the only entities willing to pay the cost and take on the risk associated with online banking.

Several steps are involved in developing a custom online financial transaction system. First, the financial institution typically selects a third party vendor to assist in the identification of hardware to be purchased as well as in the design and development of the online system. Even if the financial institution decides to develop its custom system internally, the process is daunting due to the wide range of technical platforms and the corresponding variations in cost. If a third party vendor is used, a contract between the financial institution and the vendor must be negotiated and signed before work may begin. The next step in the process is for the financial institution to work with the vendor in developing an interface into the financial institution's core processing system. This interface alone could take from 120 to 180 days to develop depending on the design and testing requirements. During system development, financial institution staff must be trained

to operate the system and to handle questions from customers. Thus, the effort to create a custom online financial transaction system from the ground up is enormous and quite costly, and this has prevented many small- and medium-sized financial institutions from being able to offer the ability to conduct online financial transactions to their customers.

SUMMARY OF THE INVENTION

The system and method of the present invention makes use of a public communications network and at least one EFT network to enable the conduct of financial transactions by a financial institution customer or debit cardholder over the networks. This is done over a secure connection without transmitting the user's PIN. The system includes a data center with at least one server and at least one database wherein the data center is connected to the communications network and to the EFT network. Also included in the system is a user interface connecting at least one authorized user to the communications network. The database is used to store data corresponding to financial transactions requested by a user that are to be processed by the server and sent over the EFT network without transmitting the user's PIN. The method of the present invention comprises a user connecting to a data center over a public communications network through a user interface. After establishing the connection, the user enters an encrypted session with the server. Next, the user securely logs into the server using an access ID and password that are validated before the user is permitted to proceed. Once validated, the user is able to conduct an online financial transaction without transmitting the user's PIN over the network.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows the major components in the present system for conducting authenticated PIN-less debits over a public communications network.

FIGS. 2A and 2B are a flowchart depicting the steps for conducting financial transactions over the system of FIG. 1.

FIG. 3 is a flowchart of the internal processing steps taken by the system of the present invention in the debit phase once the user schedules a bill for payment.

FIG. 4 is a flowchart of the submit phase of the present invention and depicts the steps taken in conjunction with a bill processor for payment of an electronic bill.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is directed to a system and method for providing online financial transaction services to financial institution debit cardholders and customers who want to access their accounts through a public communications network, such as the Internet.

As shown in Fig. 1, the system 10 of the present invention reduces the complexity, implementation time and related cost typically associated with developing a custom online financial transaction system by taking advantage of two existing systems: a public communications network 20, such as the Internet, and an EFT network 22. The term "Internet" or "web" used herein should be understood to mean any public communications network. Connected to these two existing systems is a data center 12. An interface access 28, such as a browser, with the Internet 20 permits a financial institution customer or other user 30 to log into a web site hosted on the data center 12 to conduct financial transactions such as obtaining account balances, transferring funds, and paying bills electronically through the interface 28 to the EFT network 22. The customer interface 28 resides on a secure server 14 at the data center 12. Also connected to the data center 12 is at least one database 16 for storing customer financial transactions to be processed by the system 10. In the preferred embodiment, the server 14 is DEC Alpha server 4100 although any suitable computer known in the art may be used. The database 16 used is Oracle 8 Enterprise Edition offered by Oracle, although any database running a relational database management system and a standard query language such as SQL, 4GL or C with embedded SQL can be used.

The customer interface 28 on the server 14 may be reached either through a financial institution's own web site or via a web site maintained by the EFT network provider or its third party processor. A bill payment processor 26 is also connected to the data center 12 through a communication line. The data center 12 is able to process financial transactions over the web 20 by utilizing a connection that exists between the data center 12 and the EFT network 22. In other words, a separate interface between the data center 12 and each individual financial institution 24 is not required since all the necessary financial data is obtained directly from the connection between the data center 12 and the EFT network 22. Instead of having to develop, maintain and operate a custom interface into each financial institution's core processing system, the present invention makes use of a common interface

residing on the data center 12 through which financial institution customers 30 can securely conduct their financial transactions. In this way, the amount of work needed to bring the financial institution online is reduced from an average of 150 days down to a few hours—with all the concomitant savings of time and money.

The present invention has the added advantage of being designed so that each financial institution 24 using the system 10 can rely on the security and dependability of the existing EFT network 22 for the communications backbone and authorization protocols for processing customers' financial transactions. Thus, the invention provides a simpler way to connect financial institution customers 30 to their financial institutions using personal computers or any Internet access device while maintaining the security needed for transmitting sensitive financial information.

One of the significant features of the present invention is its ability to handle online financial transactions by sending a Point of Sale ("POS") request through the EFT network 22 without sending the user's PIN. This means of sending requests to the EFT network 22 is possible since the data center 12 is a "trusted" data center. Data center authentication may be achieved by qualifying as a SAS-70 Level 2 data center through the instigation of procedures necessary to ensure that proper controls for dealing with sensitive financial information are in place so as to prevent fraud, especially in the transfer of funds, balance inquiries, and payment of bills. SAS-70 Level 2 means that the data center has passed a set of stringent security requirements and is therefore a "trusted" data center. The data center 12 validates each user 30 of the system 10 during login by verifying the customer's access ID and password. Each customer's account information is stored on the secure server 14 at the data center 12 and is uniquely identifiable through proper entry of the customer's access ID and password without use of a customer PIN. Although the customer's debit card number is included in the stored information, for security reasons the customer's PIN is not. Once the data center 12 has the necessary customer authentication, the EFT network 22 will accept requests as PIN-less POS transactions for any authorized customer 30 of any financial institution 24 that is connected to the EFT network 22. In this way, transaction requests no longer require the information normally stored in the magnetic stripe on an ATM debit card to be sent in the message stream from the data center 12 to the EFT network 22. More importantly, the magnetic stripe information does not have to be

retrieved from the financial institution 24 or stored at the data center 12 and is therefore not subject to the risk of disclosure to others.

Figs. 2A and 2B are flowcharts of the steps in the operation of the present invention to conduct financial transactions over a public communications network 20, such as the Internet, through a participating EFT network 22. As shown in Fig. 2A, the user 30, i.e., the bank customer desiring to perform an online banking transaction, launches a web browser 28 at step 32 which permits access to the public communications network 20. The browser software (not shown) must be able to handle an encrypted session between the user 30 and the data center 12. Typically, the browser runs on a personal computer, and the encrypted session is established through SSL (Secure Socket Layer) although any system for achieving an encrypted session will suffice. The specific browser software used may also vary and includes, for example, text-based browsers, EMAC browsers, Netscape™, Internet Explorer™, and Web TV™. Thus, access is not limited to that through a personal computer or web-based kiosk but may be made at any location and via any means permitting such access.

The user 30 then connects to the user interface on the data center web site at step 34. To do this, the user 30 might access his financial institution's web site or may log into a site operated by an EFT network. At step 36, the user 30 will enter an encrypted session with the secure server at the data center at which time the secure server sets a cookie on the user's browser that is used by the data center to identify the user 30 throughout the session. Next, the user 30 logs into the secure server by entering his access ID and password at step 38. If the ID and password are valid, the user 30 is presented with a main menu at step 40. If the ID and password are not valid, the system denies the user 30 access at step 42. The system may permit the user 30 a predetermined number of attempts within a specified time frame to correctly enter a valid ID and password before permanently denying access to the system at step 44.

Once the user 30 is authenticated, the user will typically have a range of options including accessing customer service at step 46, viewing accounts at step 48, reading messages from a financial institution at step 50, authorizing online bill payments at step 52, or exiting the system at step 54. Regarding messages the user 30 may receive from the system at step 50, the user is notified at the main menu 40 if there are email messages

waiting at step 56. The messages may be encrypted if they contain sensitive financial data, or they may be unencrypted email messages sent over the public communications network. If the user 30 desires, the user may read email at step 58.

Referring now to Fig. 2B, if the user 30 wants to make a bill payment using the online system, the user proceeds to the payments page at step 60 where previously entered pending bills, if any, for the user are listed and displayed. In addition, this page lists various bill pay options. To pay a new bill, the user 30 selects the option to pay a new bill at step 62.

Paying a bill requires various types of information to ensure that the user's account with the proper vendor is credited. The first step in this process is the selection of a vendor to pay. After the user 30 selects the option to pay a new bill at step 62, the user is presented with a vendor query page at step 64 where the user is prompted for information about the particular vendor to be paid (e.g., address, name, etc.). Based on the information entered, the user 30 can search a database of vendors at step 66 to see if the desired vendor already exists in the system. A list of likely vendor matches is presented to the user 30, and then the user can page through and select the desired vendor to pay at step 68. If the desired vendor does not appear in the list at step 68, the user has the option of entering the vendor into the system database at step 70. Identifying information such as the vendor's name and address is entered in the system. Based on this information, the bill processor 26 (see below) may issue a paper check to pay the vendor until such time as the vendor can be added to the system.

Next, the system of the present invention chooses a bill processing entity (such as Moneyline Express of Minneapolis, Minnesota). For each user's financial institution 24, the data center 12 maintains information regarding bill pay priorities for that institution. This information is dictated by each financial institution and includes which bill processor 26 it wishes to use—whether that be Moneyline Express or some other bill payment processor. Once a user has requested bill payment be made to a valid vendor, at step 72 the system software selects the bill payment processor 26, based on that financial institution's preferences, that is able to make a payment from the user to the specified vendor. The next step 74 in the process occurs when the user edits, adds and schedules the bill payment. Information such as bill type (one-time or recurring), period, the vendor's account number for the user, the user's bank account to be debited for payment, and memo text is added by

the user. The system may validate some or all of the information entered by the user into the system. Once the user submits the changes or adds the bill at step 78, the payment will appear on the vending payment screen (previously described at step 60) with the parameters as entered. The editing process may also be used by the user at step 76 on any pending bill displayed on the vending payment screen, including on the bill just added. The user may then add another payment, edit an existing payment, return to any of the other services on the main menu, or log off the system.

Referring now to Fig. 3, further automated processing of a bill payment by the system 10 of the present invention is illustrated. When a user schedules a bill to be paid, a debit record entry is generated and added to the database 16. The debit record entry contains all the information needed for payment of the bill through the EFT network 22. At step 80, software running at the data center periodically checks the database 16 where the pending bill payment information is stored. The software is designed to detect when a new bill has been scheduled for debiting. After detection, the software continues to monitor the bill, and when the cutoff time, determined by the financial institution 24 that holds the settlement account, is reached, the software retrieves the corresponding bill pay information from the debit record entry in the database. At step 84, the bill pay software first verifies that money is available in the account from which funds will be withdrawn. If sufficient funds are unavailable, the bill is rescheduled for payment on the following day at step 86, and a new record reflecting the revised schedule date is added to database 16 for that bill payment.

If funds are adequate to pay the bill at step 84, at step 88 the software creates and sends messages to debit the user's account and credit the settlement account, and calls the bill pay debit module to process the messages it has created. The software will also create a new bill payment record if the bill being paid is a recurring bill such as a mortgage payment. Any new bill payment record created in this way is then added to the database 16. The bill pay debit software processes the messages formed at step 88 by creating and sending encrypted messages to other software, referred to as the ATM software, that runs on the data center system at step 90. In the preferred embodiment, the messages begin as ASCII text in a generic format that is applicable to a variety of EFT networks. Each message is then encrypted with Kerberos with 3DES, developed by MIT and available from MIT under license, as it is transmitted within the system and processed by the ATM software. Each

message is then translated into the specific ISO8583 format before being sent to a particular EFT network. Use of ASCII, ISO 8583 and Kerberos with 3DES, however, are not required for messaging, and any format and/or encryption technique may be used. The ATM software will then route each message to whichever EFT network (Shazam, Pulse, Honor, etc.) the user or the user's institution utilizes. In the preferred embodiment, the ATM software is written in the C++ computer language, and the EFT network is Shazam (operated by ITS, Inc. of Johnston, Iowa). At step 92, the receiving EFT network system converts messages received from the ATM software to a format accepted by the EFT network. In this way, the ATM software is able to interface with multiple EFT networks serving financial institutions across the nation and even around the world. At this point, conventional POS processing by the EFT network takes over at step 94. In particular, the user's financial institution receives a message from the EFT network advising the financial institution to pull funds from the user's account and credit them into the settlement account typically maintained by the EFT network. The funds in the settlement account are eventually accessed by a bill payment processor, such as Moneyline Express, for actual bill payment to the various vendors to be paid as described in more detail below.

If the funds are available, the transfer occurs through the EFT network at step 96 and approval of the transaction is sent back to the originator of the request, i.e., to the data center 12 at step 98. If sufficient funds are not available, a status message is sent via the EFT network back to the data center at step 98. Either way, the database at the data center 12 is updated at step 100 with information regarding the approval or rejection of the bill payment. If the payment was rejected or an error was encountered, the bill is rescheduled for payment on the next day. If bill payment was approved, successful completion of the payment is reflected in the database records. Upon the user's next login at step 102, an encrypted message is sent to the secure server from the database informing the secure server of the status of the bill payment at step 104. The bill payment screen is then updated for viewing by the user at step 106. In this way, users are notified on the bill payment screen regarding any problems encountered in paying a bill through the system 10. That way, the user has the opportunity to correct any errors in the attempted bill payment. Furthermore, data regarding the processing of a bill is constantly logged so that the precise "path" taken by a particular bill through the system can be investigated if needed.

Whenever the database records are updated to reflect that a bill payment was properly debited in the EFT network, additional steps are required so that the bill pay processor 26 can pay the necessary vendors and so that the user will receive the necessary recognition that the user's account has been paid. As shown in Fig. 4 at step 108, a submit record is created and added to the database 16 whenever an approval for payment has been received from the EFT network. This record is similar to the debit record described earlier. The software running at the data center 12 constantly monitors the database for submit records and will gather all submit records for a particular bill payment processor 26 at step 110. Before sending a request to the payment processor, the software obtains the necessary vendor (name, address, etc.) and user (name, account with vendor to be credited, amount of payment, etc.) information. Information for all such bills to be paid by a particular bill processor are retrieved and written to a file in a format prescribed by the payment processor. This submit file is then sent to the bill payment processor 26. Once the bill processor receives the file at step 112, it processes each record in the file. As a record in the submit file is processed, the user is kept informed of the status on the bill payment screen via communication from the bill processor to the data center which is then used to update the database 16. At step 114 the bill processor debits its settlement account for the amount of the bill plus any transaction fees associated with the online bill payment, and this status is sent back to the data center 12. Next, as shown in step 116, the bill processor credits each vendor to whom money is owed, and the status of this step is relayed to the data center 12. The process is referred to as "sweeping" the money out of the many different customers' checking or savings accounts and into the settlement account.

It is intended that the description of the preferred embodiment of the present invention is but one embodiment for implementing the invention. Variations in the description likely to be conceived of by those skilled in the art still fall within the breadth and scope of the disclosure of the present invention. While specific alternatives to components of the invention have been described herein, additional alternatives not specifically disclosed but known in the art are intended to fall within the scope of the invention. It is understood that other applications of the present invention will be apparent to those skilled in the art upon the reading of the preferred embodiment and a consideration of the appended claims and drawings.

We claim:

1. An online financial transaction system for use with a public communications network and at least one EFT network to permit authorized users having PINs to conduct financial transactions over the networks with a financial institution electronically connected to the communications network and to the EFT network, the system comprising:

a data center connected to the communications network and to the EFT network, the data center further comprising:

at least one secure server;

at least one database; and

a user interface connecting at least one authorized user to the communications network wherein the database contains data corresponding to financial transactions requested by a user that are to be processed via the secure server over the EFT network without transmitting the user's PIN.

2. The system of claim 1 and further including:

a bill payment processor connected to the data center wherein authorized bill payments are made by the bill payment processor at the request of the user.

3. The system of claim 1 wherein the data center is a SAS-70 Level 2 data center.

4. A method of conducting online financial transactions over a public communications network and at least one EFT network to permit authorized users having PINs to conduct financial transactions over the networks with a financial institution electronically connected to the communications network and to the EFT network, the method comprising:

establishing a communications link to a secure data center server over the public communications network via an interface;

entering an encrypted session with the data center server;

logging into the data center server with a user's access ID and password pair;

validating the user's access ID and password pair at the data center server; and

conducting an online financial transaction without transmitting the user's PIN.

5. The method of claim 4 wherein the establishing a communications link further comprises pointing a web browser to a financial institution's web site on the Internet.

6. The method of claim 4 wherein the online banking transaction is account inquiry.

7. The method of claim 4 wherein the online banking transaction is the transfer of funds between user accounts.

8. The method of claim 4 wherein the online banking transaction is bill payment.

9. The method of claim 8 further comprising:

selecting a vendor to pay;

choosing a bill payment processor; and

adding bill payment information to the system.

10. The method of claim 9 wherein selecting a vendor further comprises entering a new vendor.

11. The method of claim 9 wherein selecting a vendor further comprises searching a vendor list stored in the data center server based on information entered by the user.

12. The method of claim 9 wherein choosing a bill payment processor is performed by the user.

13. The method of claim 9 wherein choosing a bill payment processor is accomplished by the data center server based on preferences from a financial institution.

14. The method of claim 9 wherein the bill payment information comprises a bill type, a period for bill payment, a vendor-user account number, and a user bank account number.

15. The method of claim 9 further comprising validating the bill payment information.

16. The method of claim 9 wherein adding bill payment information further comprises:

editing the bill payment information; and

scheduling a bill payment.

17. The method of claim 9 further comprising:

generating a new debit record entry corresponding to the bill payment information;

detecting the new debit record entry;

monitoring the new debit record entry until a cutoff time is reached;

retrieving bill payment information from the debit record entry;

verifying that sufficient funds are available to pay the bill;

sending messages corresponding to the bill payment information to debit a user's account and credit a settlement account; and

processing the messages for bill payment.

18. The method of claim 17 further comprising:

updating the database regarding the status of the bill payment.

19. The method of claim 17 wherein data regarding the status of the bill payment is logged in the system.

20. The method of claim 17 wherein the messages are encrypted and sent to an EFT network.

21. The method of claim 17 wherein processing messages occurs over a POS system.

22. The method of claim 17 wherein processing messages further includes sending a message to the user's financial institution to debit funds from the user's account and to credit funds to an EFT network settlement account.

23. The method of claim 22 further comprising accessing the funds in the EFT network settlement account for bill payment to designated vendors.

24. The method of claim 23 wherein accessing the funds is performed by the bill payment processor.

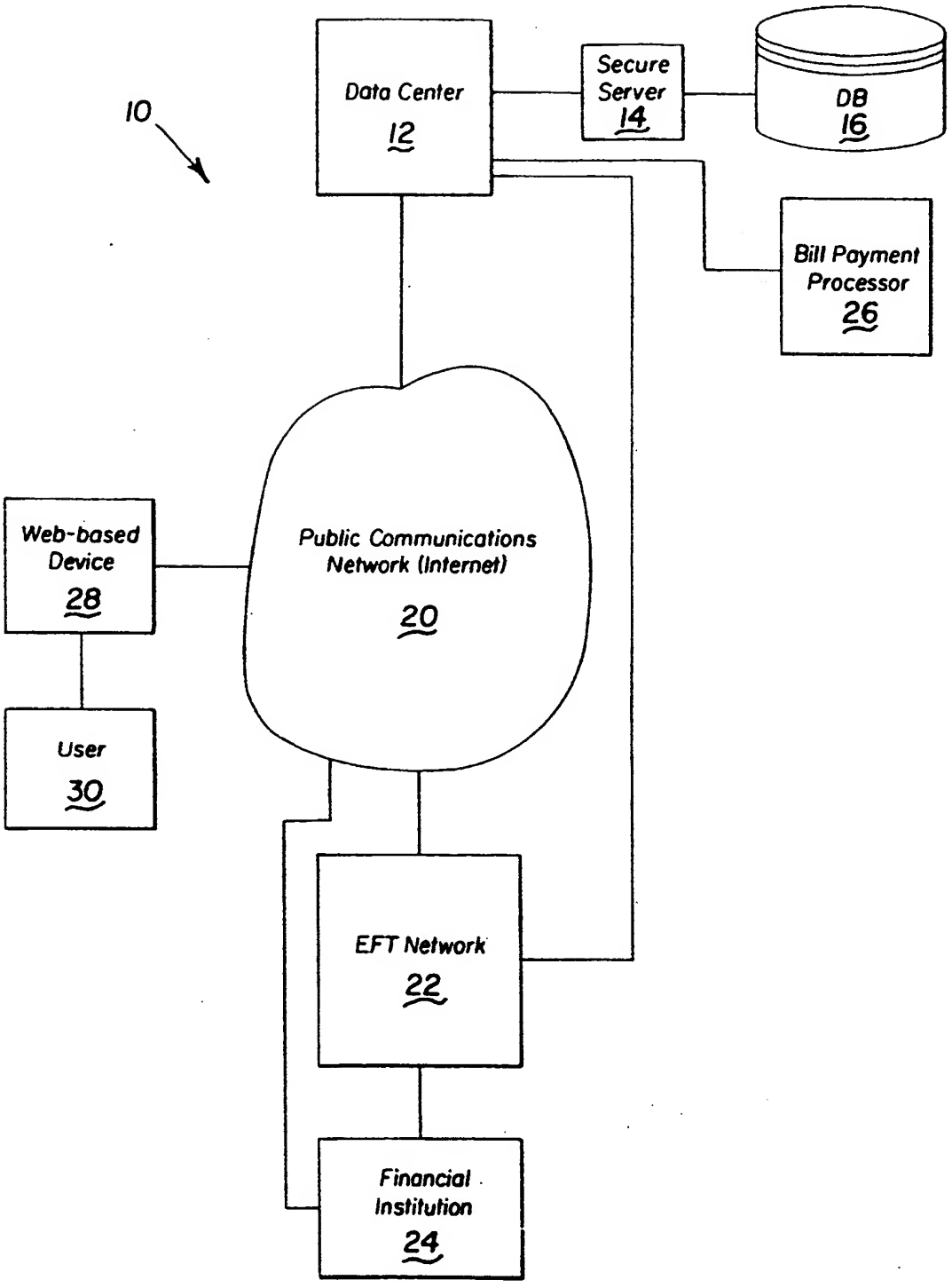

10
Data Center
12
Secure
Server
14
DB
16
Bill Payment
Processor
26
Public Communications
Network (Internet)
20
Web-based
Device
28
User
30
EFT Network
22
Financial
Institution
24

Fig. 1

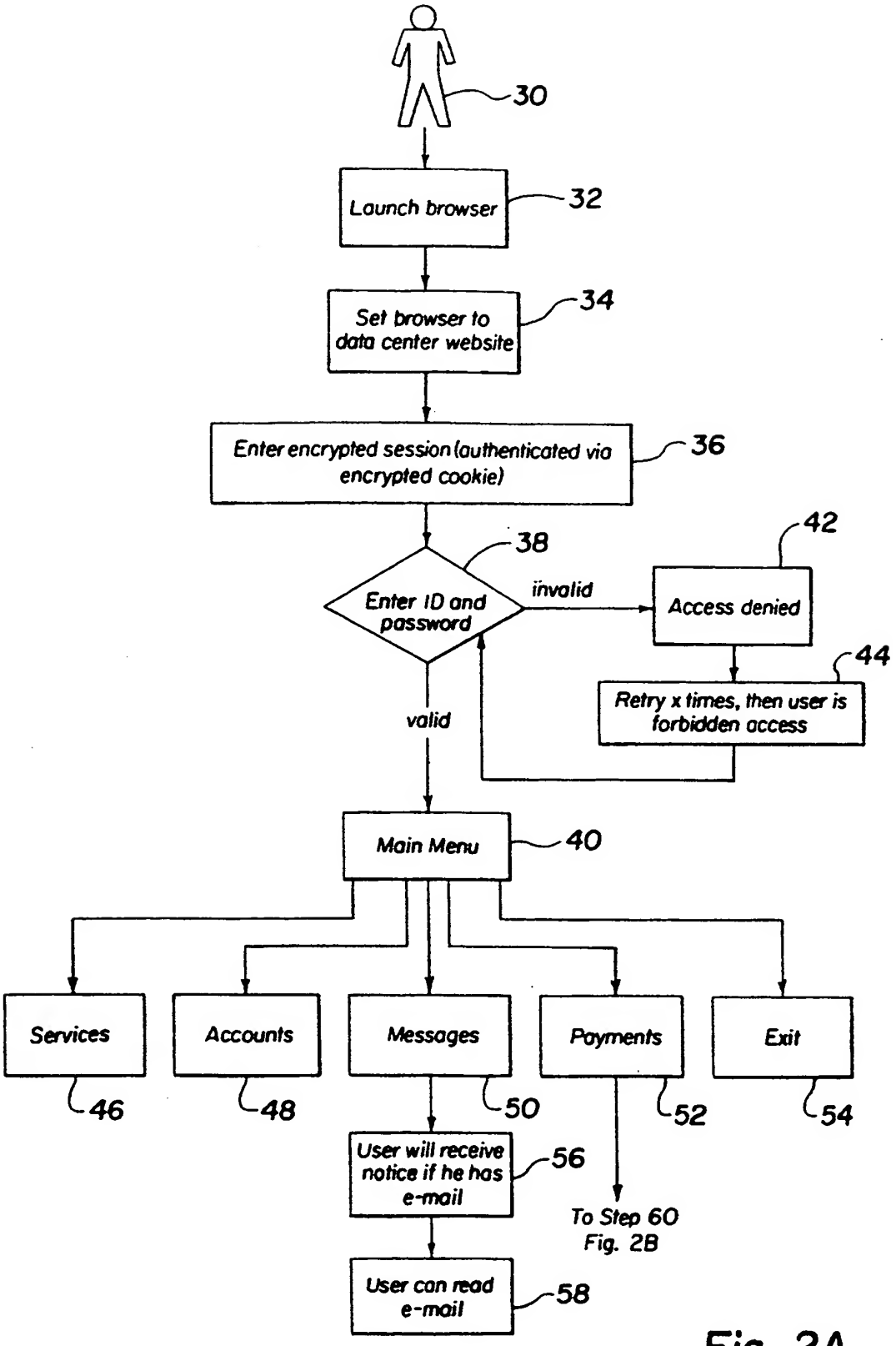

30
Launch browser
32
Set browser to data center website
34
Enter encrypted session (authenticated via encrypted cookie)
36
38
Enter ID and password
invalid
42
Access denied
44
Retry x times, then user is forbidden access
valid
Main Menu
40
Services
Accounts
Messages
Payments
Exit
46
48
50
52
54
User will receive notice if he has e-mail
56
To Step 60 Fig. 2B
User can read e-mail
58

Fig. 2A

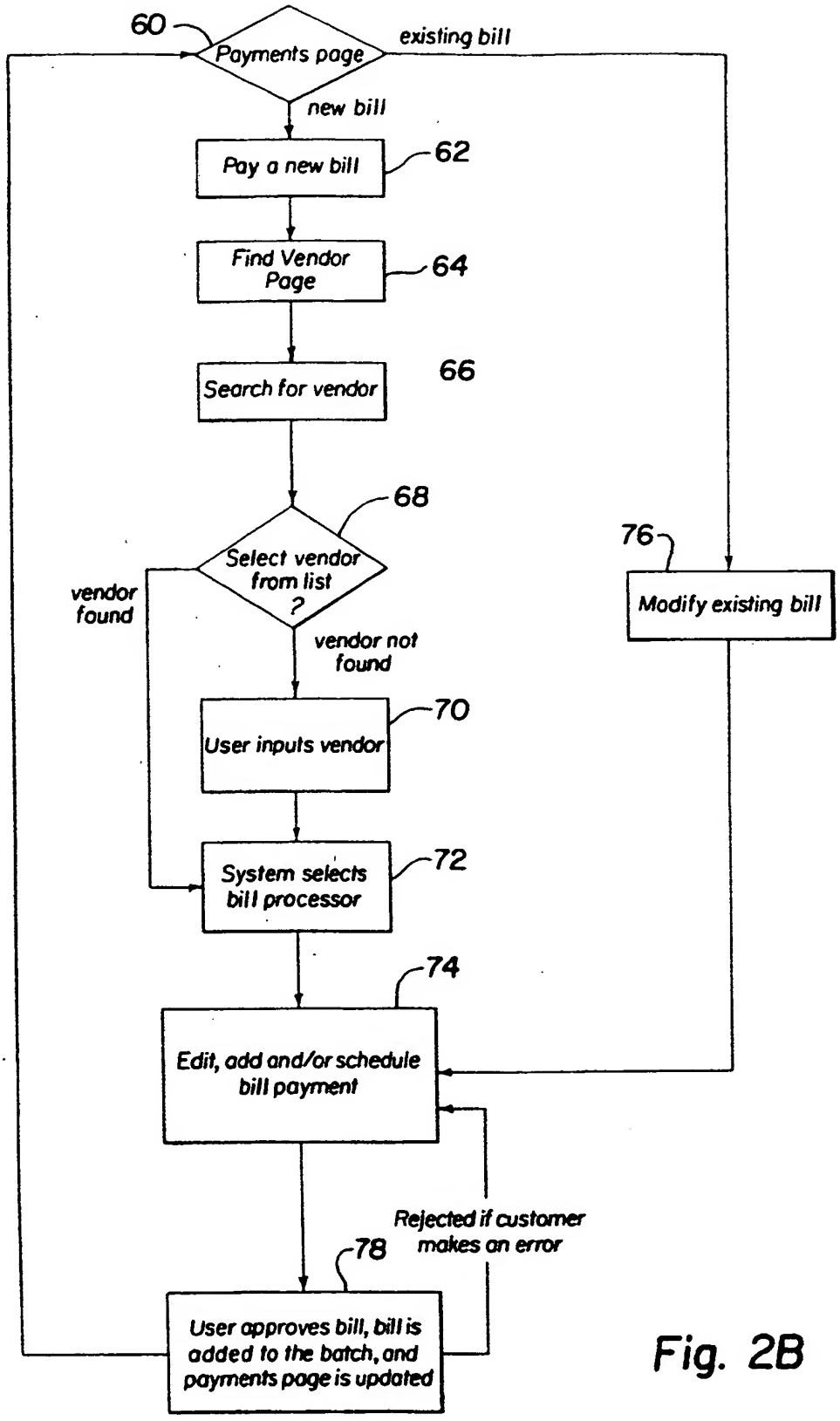

60
Payments page
existing bill
new bill
Pay a new bill
62
Find Vendor Page
64
Search for vendor
66
68
Select vendor from list ?
vendor found
vendor not found
76
Modify existing bill
User inputs vendor
70
System selects bill processor
72
74
Edit, add and/or schedule bill payment
Rejected if customer makes an error
78
User approves bill, bill is added to the batch, and payments page is updated

Fig. 2B

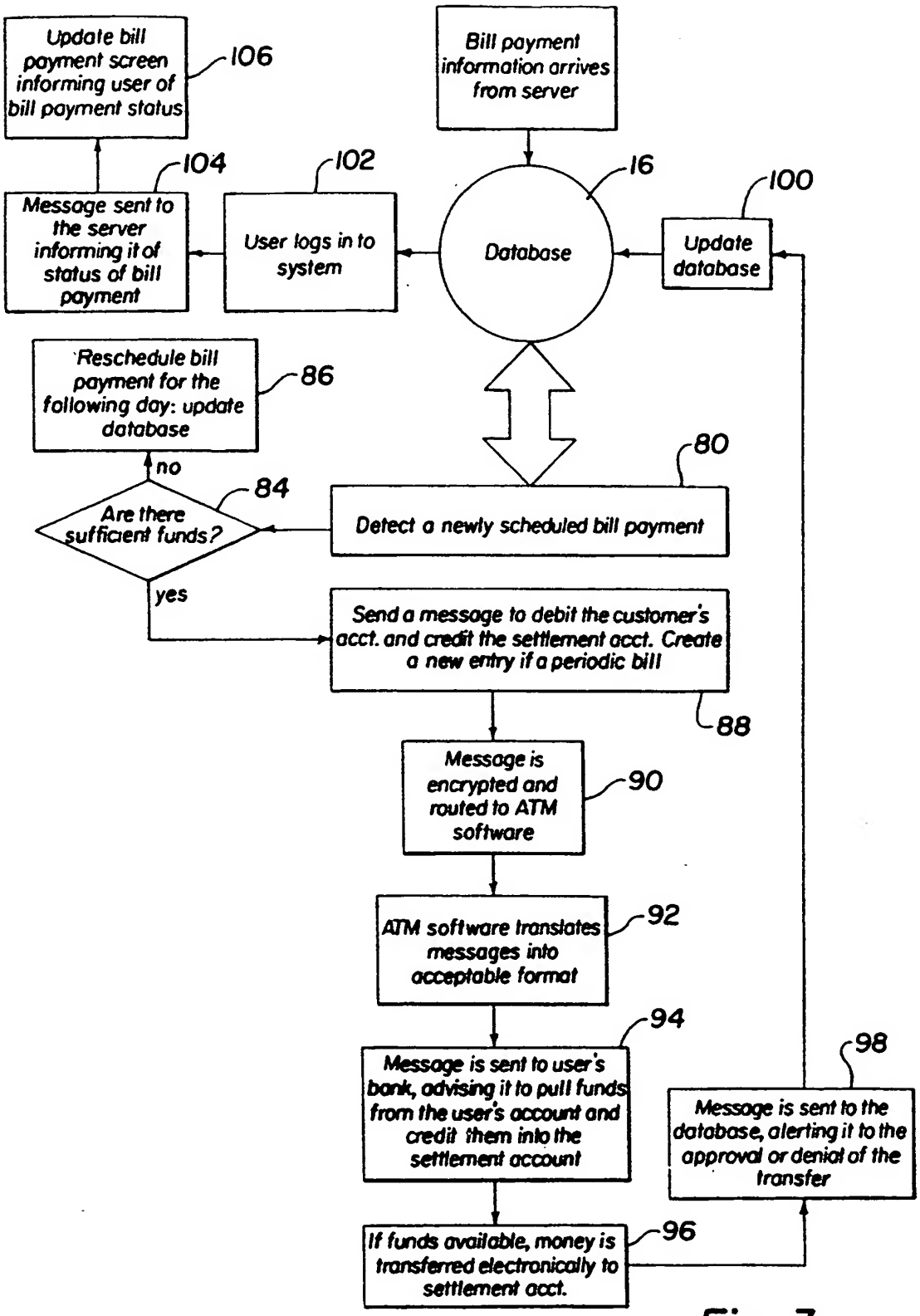

Update bill payment screen informing user of bill payment status
106
Bill payment information arrives from server
Message sent to the server informing it of status of bill payment
104
User logs in to system
102
Database
16
Update database
100
Reschedule bill payment for the following day: update database
86
no
Are there sufficient funds?
84
Detect a newly scheduled bill payment
80
yes
Send a message to debit the customer's acct. and credit the settlement acct. Create a new entry if a periodic bill
88
Message is encrypted and routed to ATM software
90
ATM software translates messages into acceptable format
92
Message is sent to user's bank, advising it to pull funds from the user's account and credit them into the settlement account
94
Message is sent to the database, alerting it to the approval or denial of the transfer
98
If funds available, money is transferred electronically to settlement acct.
96

Fig. 3

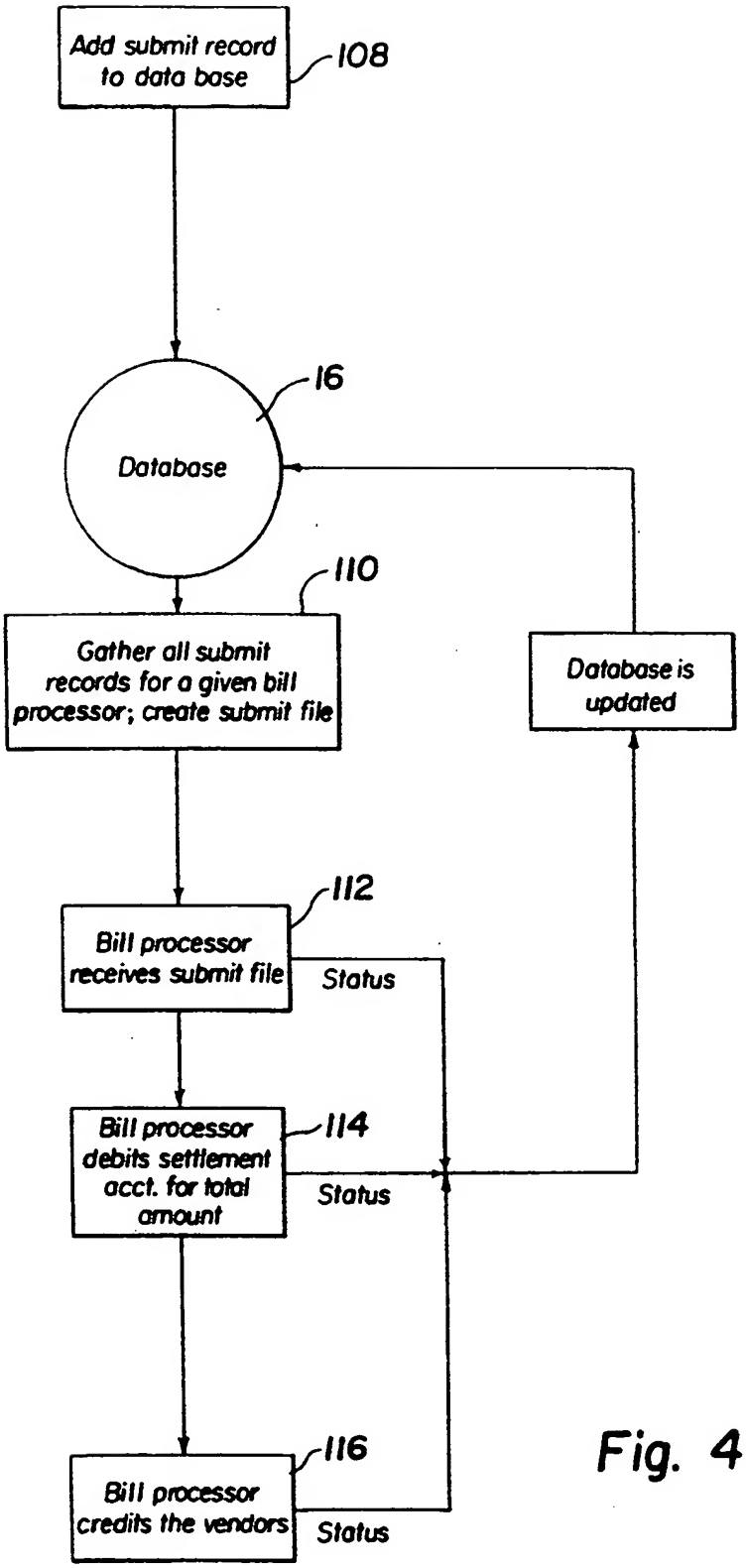

Add submit record to data base
108
16
Database
110
Gather all submit records for a given bill processor; create submit file
Database is updated
112
Bill processor receives submit file
Status
Bill processor debits settlement acct. for total amount
114
Status
116
Bill processor credits the vendors
Status

Fig. 4

INTERNATIONAL SEARCH REPORT

Int[illegible]tional application No.
PCT/US00/03017

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) : G06F 17/60
US CL : 705/35, 40, 42
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/35, 40, 42

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST, DIALOG, Corporate ResourceNet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,899,982 A (RANDLE) 04 May 1999 (04.05.1999), column 1, lines 11-25, column 2, lines 31-49, column 3, lines 29-37, column 4, lines 58-62, column 8, lines 53-55, figure 1.	1-24
Y	US 5,465,206 A (HILT et al) 07 November 1995 (07.11.1995), column 10, lines 49-62, column 15, lines 2-6, column 21, lines 1-6, column 21, lines 30-39.	1-24
A	US 5,677,955 A (DOGGETT et al) 14 October 1997 (14.10.1997), abstract.	1-24
A	STONE, B. et al. Point, Click and Pay. Newsweek. 17 August 1998, Vol 132. Issue 7, pages 66-67.	1-24
A	SHEPHERD, S. Consumers Alter Their Banking Options At the Touch of a Finger. Business Press. 24 July 1998, Vol 11. Issue 12, pages 15-16.	1-24
A, E	US 6,032,133 A (HILT et al) 29 February 2000 (29.02.2000), column 10, lines 50-63, column 14, lines 66-67, column 15, lines 1-3, column 20, lines 66-67, column 21, lines 27-36.	1-24
A	US 5,774,663 A (RANDLE et al) 30 June 1998 (30.06.1998), abstract.	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
11 May 2000 (11.05.2000)

Date of mailing of the international search report
29 JUN 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
Robert A. Weinhardt
Joni Hill
Telephone No. (703) 305-9780

Form PCT/ISA/210 (second sheet) (July 1998)